SECURITY PROTECTION MODULE FOR TELECOMMUNICATION

Publication number: JP7303139

Publication date: 1995-11-14

Inventor: DEBITSUDO TEIMOSHII GUSUTAFUSO; MAIKERU AREN SABEEJI; POORU ROI KENEDEI; JIYOSEFU KITSUSHIYU ZA SAADO; BURUUSU ARAN FUETSUTE

Applicant: MOTOROLA INC

Classification:

- international: ***H04K1/06; H04L9/00; H04M1/68; H04Q7/38;*** *H04Q7/32;* **H04K1/06; H04L9/00; H04M1/68; H04Q7/38;** H04Q7/32; (IPC1-7): H04M1/68; H04K1/06; H04Q7/38

- European: H04L9/00

Application number: JP19950124509 19950426

Priority number(s): US19940234793 19940428

Also published as:

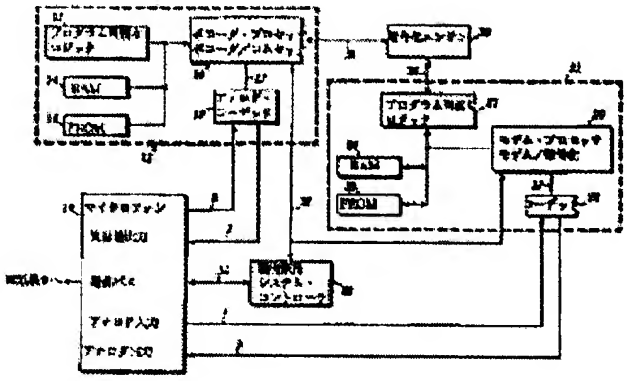
EP0680171 (A2)

US5524134 (A1)

EP0680171 (A3)

Abstract of **JP7303139**

PURPOSE: To provide a miniaturized and power-consumption saving module by supplying no power to a processor subsystem of a security module, while a telephone set is in a standby mode. CONSTITUTION: A security system controller 29 monitors an external communication bus 34 and an internal communication bus 32 inside a portable radio telephone set. Until a suitable instruction string is detected on the bus 34, a vocoder processor 10 and a modem processor 20 are held in an idle mode. When a suitable instruction string is detected, power is supplied to a vocoder/comsec subsystem processor 11 and a modem/signaling subsystem processor 20, and a security channel with a remote device for communicating with a cellular telephone set is set. Thus, power consumption is reduced, and miniaturization is attained.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平7－303139

(43)公開日　平成７年(1995)11月14日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｍ　1/68				
Ｈ０４Ｑ　7/38				
Ｈ０４Ｋ　1/06				
			Ｈ０４Ｂ　7/26　１０９　Ｒ	

審査請求　未請求　請求項の数３　ＦＤ　（全５頁）

(21)出願番号　特願平7－124509

(22)出願日　平成７年(1995)４月26日

(31)優先権主張番号　２３４７９３

(32)優先日　1994年４月28日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009597
モトローラ・インコーポレイテッド
MOTOROLA　INCORPORATED
アメリカ合衆国イリノイ州シャンバーグ、イースト・アルゴンクイン・ロード1303

(72)発明者　デビッド・ティモシー・グスタフソン
アメリカ合衆国アリゾナ州ギルバート、ウエスト・サンド・ヒルス・コート1202

(72)発明者　マイケル・アレン・サベージ
アメリカ合衆国アリゾナ州チャンドラー、ウエスト・イバンホエ・コート4182

(74)代理人　弁理士　本城　雅則　（外１名）

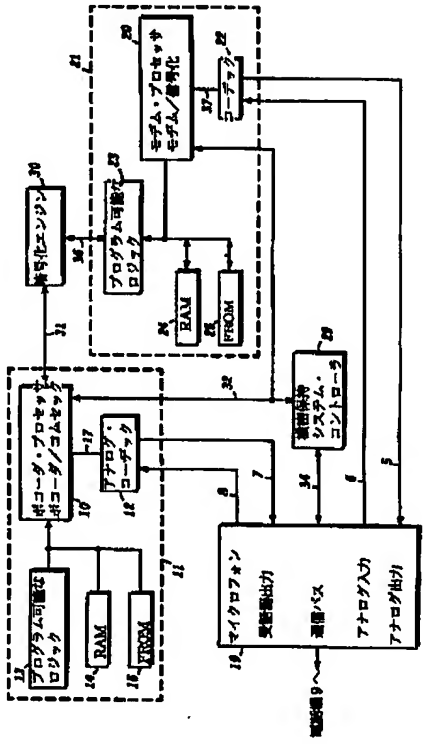
最終頁に続く

(54)【発明の名称】　遠隔通信用機密保護モジュール

(57)【要約】

【目的】　セルラ電話機用低電力消費型機密保護モデュールを提供する。

【構成】　前記機密保護モデュールは、電話機のマイクロホンからの信号および電話機の受話器への信号を処理するボコーダ・プロセッサ（１０）、暗号化エンジン（３０）、セルラ電話機からの送信および受信データを制御するモデム・プロセッサ（２０）、および機密保護システム・コントローラ（２９）を含む。前記プロセッサは、電話機が待機モードにある時は実際上全く電力を消費せず、前記セルラ電話機が動作中でも暗号化通信を行うために消費する電力は極くわずかである。



1

【特許請求の範囲】

【請求項1】　電話機用機密保護モジュールであって：デジタル音声データの圧縮および伸張を提供する第1プロセッサ（11）；前記圧縮および伸張デジタル音声データの暗号化および暗号解読を行う暗号化エンジン（30）であって、前記第1プロセッサに結合される前記暗号化エンジン；暗号化されたデジタル圧縮音声データを、暗号化されたアナログ圧縮音声データに変換すると共に、暗号化されたアナログ圧縮音声データを暗号化されたデジタル圧縮音声データに変換する第2プロセッサ（21）であって、前記暗号化エンジンに結合される前記第2プロセッサ；および状態信号を送出し、前記第1および第2プロセッサの動作を制御する命令を受信する機密保護システム・コントローラ（29）；から成ることを特徴とする機密保護モジュール。

【請求項2】　セルラ電話機用機密保護モジュールであって：デジタル音声データの圧縮および伸張を提供する第1プロセッサ（11）；前記圧縮および伸張デジタル音声データの暗号化および暗号解読を行う暗号化エンジン（30）であって、前記第1プロセッサに結合される前記暗化エンジン；暗号化されたデジタル圧縮音声を暗号化されたアナログ圧縮音声に変換すると共に、暗号化されたアナログ圧縮音声を暗号化されたデジタル圧縮音声に変換する第2プロセッサ（21）であって、前記暗号化エンジンに結合される前記第2プロセッサ；および状態信号を送出し、前記第1および第2プロセッサの動作を制御する命令を受信する機密保護システム・コントローラ（29）；を含むことを特徴とする機密保護モジュール。

【請求項3】　セルラ電話機用機密保護モジュールであって：デジタル音声データの圧縮および伸張を提供する第1プロセッサ（11）；前記圧縮および伸張デジタル音声データの暗号化および暗号解読を行う暗号化エンジン（30）であって、前記第1プロセッサに結合される暗号化エンジン；暗号化された圧縮デジタル音声を暗号化された圧縮アナログ音声に変換すると共に、暗号化された圧縮アナログ音声を暗号化された圧縮デジタル音声に変換する第2プロセッサ（21）であって、前記暗号化エンジンに結合される第2プロセッサ；および状態信号を送信し、前記第1および第2プロセッサの動作を制御する命令を受信する機密保護システム・コントローラ（29）；から成ることを特徴とするセルラ電話機用機密保護モジュール。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は機密保護遠隔通信に関し、更に特定すれば、セルラ遠隔通信用機密保護システムに関するものである。

【0002】

【従来の技術】現在の機密保護電話機の市場は、主として、アナログ電話線を用いる公衆電話交換網(public switched telephone network)での運用に関係するものである。現在、機密保護用電話製品は、多くの異なる技術（ボコーダ(Vocoder)、モデム、信号化(Signaling)、および暗号化(Encryption)）で構成され、かなりの量の電力を消費する。

2

【0003】携帯通信が広く普及したことに伴い、電池の寿命が重要な問題となる。セルラ電話機のような遠隔通信端末に回路を付加すると、電池の寿命およびそれに従う電話機の使用に重大な影響を与える。音声通信に対する機密保護は、特に通信が容易に傍受され得る無線電話機に非常に望まれるものである。しかしながら、機密保護用回路を付加すると、無線電話機の寿命およびそれに従う無線電話機の送受信に用いられる機能に影響を与えることになる。

【0004】電池の寿命は、機密保護通信を使用して命令する米国政府における多くの用途（即ち、保護(covert)、調査、救命等）にとって、非常に重要な特別なパラメータ(critical mission parameter)である。商用でも同様に、機密保護通信を必要とする場合には、無線電話機の人間工学に対する基本的な要求（即ち、小型、携帯可能であること、等）がある。

【0005】遠隔通信端末用の一般的な機密保護モジュールには、機密保護対象の装置および目標の通信媒体に直列に配置される付属品がある。従来技術の例には、すでに商業市場(marketplace)において認められる単純な古い電話機用の機密保護モジュール，ファックス機器，および機密保護モデム(secure modem)がある。

【0006】これら一般的な機密保護システムは、携帯性や小型化が考慮されない。これらの問題は、通常、大型電池を提供することによって、ここではＤＣ－ＤＣコンバータとしてとらえられる、適正な電力出力が提供され克服される。これらの装置を収容(packaging)するには、常にブリーフケースや、小型の携帯用搬送装置が用いられる。

【0007】

【発明が解決しようとする課題】小型で消費電力を低減した、セルラ電話機用機密保護モジュールを提供することである。

【0008】

【課題を解決するための手段】本発明の機密保護モジュールは、電話機のマイクロフォンからの信号および電話機の受話器への信号を処理するボコーダ・プロセッサ，暗号化エンジン、セルラ電話機からの送信および受信データを制御するモデム・プロセッサ，および機密保護システム・コントローラを含む。前記プロセッサは、電話機が待機モードにある時は実際上全く電力を消費せず，前記セルラ電話機が動作中でも暗号化通信を行うために消費する電力は極くわずかである。

【0009】

3

【実施例】遠隔通信端末用機密保護モジュールは、3ボルト(3volt)技術，多機能ＤＳＰ（デジタル信号プロセッサ），プログラム可能な暗号化，およびアーキテクチャの電力をできるだけ低く保つスマート電力コントローラを使用する低電力アーキテクチャを作り出すことによって、達成することができる。

【００１０】機密保護モジュールは、音声圧縮,(voice compression) 暗号化，およびモデム技術を用いて、音声のデジタル暗号を提供する。以下のブロック図は、この機密保護モジュールを示す。

【００１１】図１を参照して、本発明の好適な実施例による携帯電話用機密保護モジュールのブロック図が示される。この機密保護モジュールは、ボコーダ／コムセック・サブシステム・プロセッサ(vocoder / comsec subsystem processor)１１，暗号化エンジン(encryption engine)３０，モデム／信号化サブシステム・プロセッサ(Modem / Signaling subsystem processor)２１，および機密保護システム・コントローラ２９の４つの主なサブシステムで構成される。これらのいずれかまたは全ては、単一の大規模集積回路に統合することができる。

【００１２】ボコーダ・プロセッサ１０は、プログラム可能なロジック１３，ＲＡＭ１４,およびフラッシュＲＯＭ１５，並びにアナログ・コーデック(analog codec)１２に結合される。ボコーダ・プロセッサ１０は、暗号化エンジン３０に更に結合される。

【００１３】モデム・プロセッサ２０は、モデム・ロジック２３，RAM２４，フラッシュROM２５，コーデック２２，および暗号化エンジン３０に結合される。モデム・プロセッサ２０は、機密保護システム・コントローラ２９にさらに結合される。

【００１４】電話機９のマイクロフォン（Ｍｉｃ）と受話器出力（Ｅａｒ　ｏｕｔ）は、アナログ・コーデック１２に結合される。機密保護システム・コントローラ２９は、セルラ電話機による通常のデータ送受信のために、セルラ電話機９の通信バスに結合される。セルラ電話機９へのアナログ入力およびアナログ出力は、コーデック２２に結合される。

【００１５】ボコーダ／コムセック・サブシステム１１は、音声信号の圧縮／伸張のために用いられると共に、全体の機密保護機能のいくつかを行う。これは、デジタル信号プロセッサ１０，メモリ即ち、フラッシュ・リード・オンリ・メモリ（ＦＲＯＭ）１５およびランダム・アクセス・メモリ（ＲＡＭ）１４，プログラム可能なロジック１３，およびA／D（アナログからデジタル）およびD／A（デジタルからアナログ）変換を行うアナログ・コーデック１２を含む。ボコーダ・プロセッサ１０は、フラッシュ・リード・オンリ・メモリ１５とランダム・アクセス・メモリ１４とを用いて、音声圧縮および伸張計算を行い、通信機密保護（コムセック）メッセージを暗号化エンジン３０に送出する。全てのプログラム

4

は、ＦＲＯＭ１５からダウンロード(download)され、ＲＡＭ１４を用いて実行される。プログラム可能なロジック１３は、メモリとボコーダ・プロセッサ１０との間でメモリ・複号化を行う。プログラム可能なロジック１３は、将来の機能拡張も考慮したものである。ホスト・ポート３１は、ボコーダ・プロセッサと暗号化エンジンとの間の通信路である並列ポート(parallel port)である。

【００１６】暗号化エンジン３０は、圧縮された音声信号について、暗号化および暗号解読を行うために用いられる。これは、ボコーダ・プロセッサ１０および暗号化および暗号解読のためのメモリと異なるソフトウエア・アルゴリズムを用いてプログラムされるＡＳＩＣ（Application Specific Integrated Circuit：特定用途集積回路）のような低電力のプログラム可能なロジックである。暗号化エンジンは、２本の異なる経路を介して通信する。この２本の経路とは、（1）圧縮された明瞭なテキスト音声信号の暗号化／暗号解読のために、ボコーダ・プロセッサ１０に（ホスト・ポート３１を介して）通信する経路；および（2）モデム・プロセッサ２０によってソフトウエア的に実行されるモデムのデータ・ポンプ(datapump)との間で暗号化した圧縮音声を送信／受信するために、モデム・プロセッサ２０に（プログラム可能なロジック２３を介して）通信する経路である。

【００１７】モデム／信号化サブシステム２１は、アナログ・チャネルを超じた搬送のために、暗号化された圧縮音声信号の変調／復調を行う。これは、デジタル信号プロセッサ２０，メモリ（フラッシュ・リード・オンリ・メモリ２５およびランダム・アクセス・メモリ２４），プログラム可能なロジック２３，およびアナログ・コーデック２２（A／DおよびD／A変換を行う）を含む。モデム・プロセッサ２０は、フラッシュ・リード・オンリ・メモリ２５とランダム・アクセス・メモリ２４とを用いて、モデム計算およびモデム・トラフィックからの信号メッセージの挿入／除去を行う。全てのプログラムは全てＦＲＯＭ２５からダウンロードされ、ＲＡＭ２４を用いて実行される。プログラム可能なロジック２３は、メモリとモデム・プロセッサ２０との間でメモリ複号化を行う。プログラム可能なロジック２３は、モデムの位相ロック・ループ機能のいくつかも行う。プログラム可能なロジックは、部品数の減少および全体の電力の低減に効果がある。

【００１８】機密保護システム・コントローラ２９は、機密保護モジュールのモードを監視および制御するために用いられる６８ＨＣ１１のような単一チップのマイクロ・コントローラである。これは、（1）携帯無線電話機内に配置される外部通信バス３４，および（2）機密保護モジュールの状態を判定すると共にいつ電力を保存するかを決定するための内部通信バス３２の、２本のバスを監視する。

5

【００１９】プログラム可能なロジック・ユニット１３，２３は、Ｘｉｌｉｎｘ社によって製造されるＸＣシリーズ・プログラム可能なロジックまたはその同等品、或いは同等のゲート・アレイまたは小規模論理素子の集合によって構成することができる。コーデック１２，２２は、Ｔｅｘａｓ　Ｉｎｓｔｒｕｍｅｎｔｓ　Ｃｏｒｐｏｒａｔｉｏｎによって製造されるコーデック・ユニットTLC320AC01またはその同等品で構成することができる。プロセッサ１０，２０は、Ｍｏｔｏｒｏｌａ社製５６００２デジタル信号プロセッサ（ＤＳＰ）またはその同等品で構成することができる。フラッシュ・リード・オンリ・メモリは、ＥＥＲＯＭ，ＲＯＭまたはその同等品で置き換えることもできる。暗号化エンジン３０は、Ｍｏｔｏｒｏｌａ社製のゲート・アレイであり、次のアルゴリズム、タイプ（１）政府機密扱い(government classified)；タイプ（２）ＳｋｉｐｊａｃｋまたはＣｌｉｐｐｅｒのような政府請負業者(contractors)／警察；タイプ（３）商用はＤＥＳ（data encryption standard：データ暗号化標準）；およびタイプ（４）海外はＤＶＩ（Ｍｏｔｏｒｏｌａ　所有）またはその他の専有アルゴリズム(proprietaryalgorithms)を実行することができる。

【００２０】機密保護システム・コントローラ２９は、通信バス３４上で適当な命令列(command sequence)を検出するまで、両方のプロセッサ・サブシステム（１１，２１）をアイドル・モードに保持する。

【００２１】一旦適当な命令列が検出されると、これらサブシステムは給電され、遠くにある端末装置(far end unit)、即ち、セルラ電話機と通信する遠隔装置との機密保護チャネルを設定する。一旦機密保護チャネルが設定されると、無線電話機のマイクロフォンからの音声信号が処理される。

【００２２】無線電話機のマイクロフォンからの音声信号は、コネクタ１９上で受信される。ｍｉｃ信号８はコーデック１２に送られ、デジタル化される。デジタル化された信号は、高速直列通信バス１７を介して、プロセッサ１０に提供される。デジタル化された音声情報は圧縮され、ホスト・インタフェース・バス３１を介して、暗号化のために暗号化エンジン３０に送られる。暗号化された音声は、プロセッサ２０に供給され（シリアル通信インターフェイス３６を介して）、送信のために変調される。圧縮され，暗号化され，更に変調された音声は、コーデック２２に提供され（直列通信インタフェース３７を介して）、アナログ信号に変換され、コネクタ１９上のアナログ出力５を介して、セルラまたは携帯電話機に送信される。

【００２３】同時に、携帯電話機からのアナログ信号（遠くの端末装置のマイクロフォンからの信号）は、コネクタ１９のアナログ入力(analog In)６で受信され、コーデック２２に送られ、ここでデジタル化され、プロセッサ２０に（直列通信インタフェース３７を介して）提供される。これらの信号は復調され、暗号化エンジン３０に送られ（シリアル通信インタフェース３６を介して）、暗号解読される。暗号解読された圧縮音声情報は、次に暗号化エンジン３０からプロセッサ１０に（ホスト・インタフェース・バス３１を介して）提供され、ここで伸張される（合成される）。伸張されたデジタル音声は、アナログ・コーデック１２に（シリアルインタフェース１７を介して）送られ、アナログ音声信号に逆変換される。アナログ音声信号は、アナログ・コーデック１２からコネクタ１９に送出され（線７を介して受話器出力に入力される信号）、無線電話機の受話器に送られる。

6

【００２４】図２を参照して、本発明による機密保護低電力セルラ電話機４５の等幅図が示される。機密保護モジュール４０が、電池パック５０とセルラ電話機９との間のセルラ無線電話機９に取り付けられる。これにより、機密保護モジュールが電池から電力を受け(draw from)、セルラ無線電話機９の内部通信バスを用いることができるようになる。別個のマイクロフォンと受話器とを外部に付加し、いずれのモードでも動作できるようにしてもよい。

【００２５】機密保護セルラ電話機４５は、セルラ電話機９，図１で説明した機密保護モジュール４０，および電池５０を含む。機密保護モジュール４０は、セルラ電話機９と電池５０との間に結合される。

【００２６】機密保護モジュール４０は、接続インタフェース（図示せず）を介して、セルラまたは携帯無線電話９に接続する。接続インタフェースは、ハンドセット・インタフェース用マイクロフォンおよびイヤホン信号，無線電話機のトランシーバ・インタフェース用アナログ入出力線（５，６），および無線電話機を監視するための通信バス・インタフェース（３４）を含む。

【００２７】遠隔通信端末用機密保護モジュールは、要注意の情報(protect sensitive)および機密扱いの情報(classified information)が無線(air waves)を通じて傍受されるのを防ぐ方法を提供するので、当技術では重要な進歩である。無線技術を用いて通信する製品が増々増加しつつあるので、機密保護モジュールに対する必要性は、ユーザの意識の高まりと共に増大するであろう。更に、ここで示した構成は、セルラまたは携帯電話に低電力機密保護装置を供給し、しかもかかる電話機の電池の寿命に悪影響を与えないという、業界の要求を満足するものである。

【００２８】本発明の好適実施例を示し、その形式を詳細に説明したが、本発明の精神或いは特許請求の範囲から逸脱することなく、種々の変更が可能であることは、当業者には容易に理解できよう。

【図面の簡単な説明】

【図１】本発明による遠隔通信機密保護モジュールのブ

7

ロック図である。

【図2】本発明の好適な実施例による機密保護モジュールおよび電話機を示す等幅図である。

【符号の説明】

9　電話機

10　ボコーダ・プロセッサ

11　ボコーダ／コムセック・サブシステム・プロセッサ

12　アナログ・コーデック

8

13　プログラム可能なロジック

14，24　RAM

15，25　フラッシュROM

20　モデム・プロセッサ

21　モデム／信号化サブシステム・プロセッサ

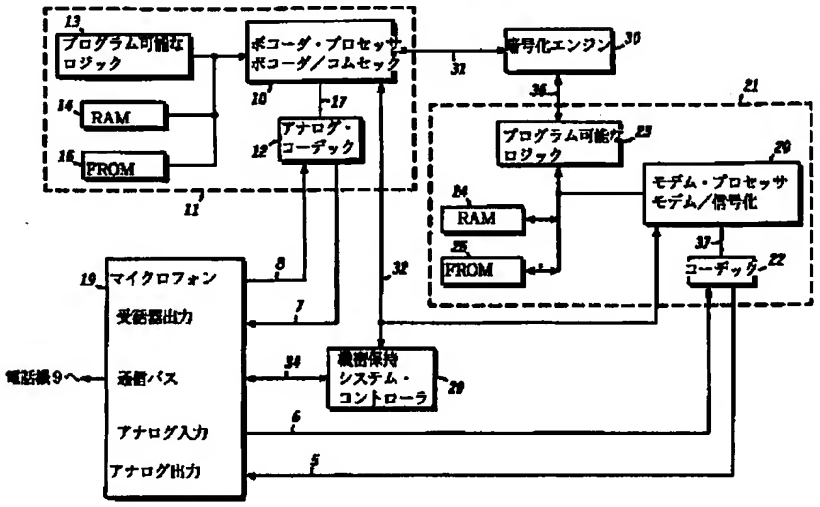
22　コーデック

23　モデム・ロジック

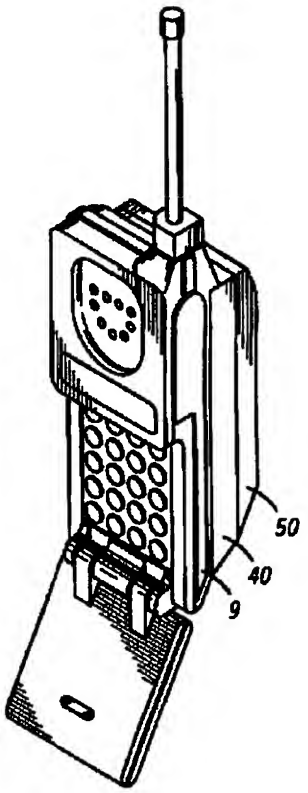
29　機密保護システム・コントローラ

30　暗号化エンジン

【図1】



【図2】



フロントページの続き

(72)発明者　ポール・ロイ・ケネディ
アメリカ合衆国アリゾナ州メサ、サウス・サラトガ2441

(72)発明者　ジョセフ・キッシュ，ザ・サード
アメリカ合衆国アリゾナ州ギルバート、ノース・オスプレイ・コート1009

(72)発明者　ブルース・アラン・フェッテ
アメリカ合衆国アリゾナ州メサ、ウエスト・デル・キャンポ2310